VPN
Virtual Private Network

國立陽明交通大學資工系資訊中心

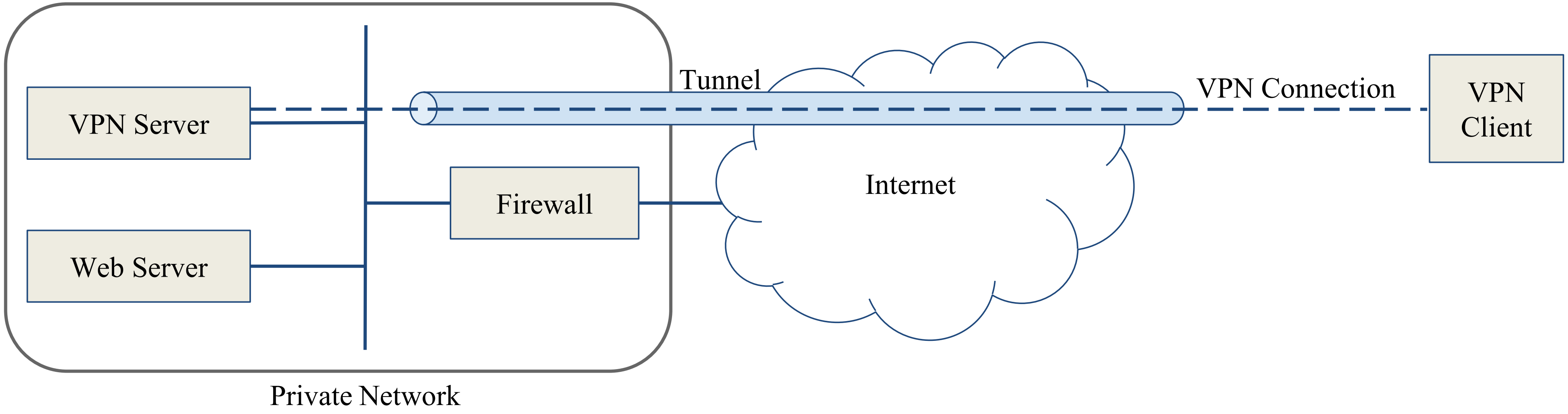
Computer Center of Department of Computer Science, NYCU

Introduction

- Uses public telecommunication channels, such as the Internet or other network service, instead of leased lines channels.
- Described as Virtual because it is distant connection using private connections.
- Used to widely now because of today's globalization.
- Connects users or branches.
- Used to use dial-up or Leased communication, now using IP-VPN’s

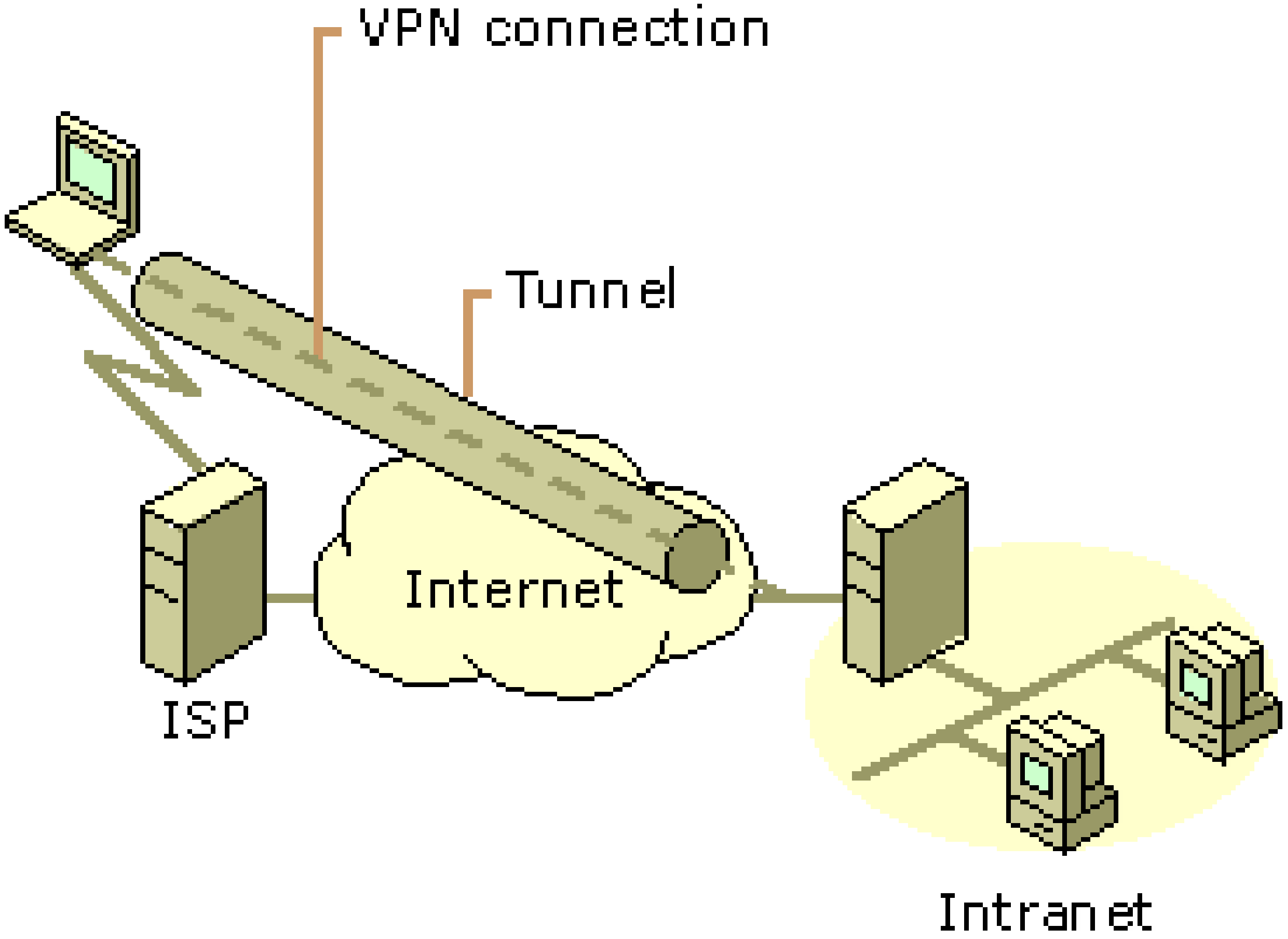
What is VPN

- Extension of a private network that encompasses links across shared or public networks like the Internet.
- Enable to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link.



Common Uses of VPNs (1/3)

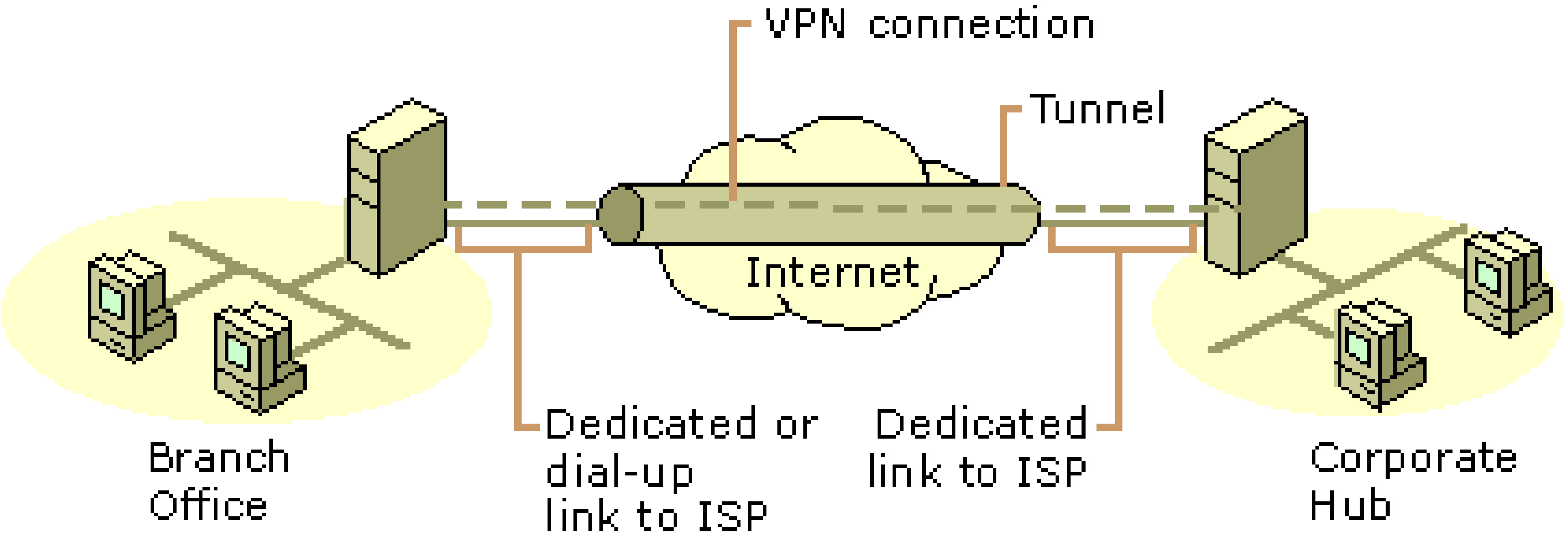
1. Remote Access Over the Internet



Virtual Private Networking: An Overview | Microsoft Docs

Common Uses of VPNs (2/3)

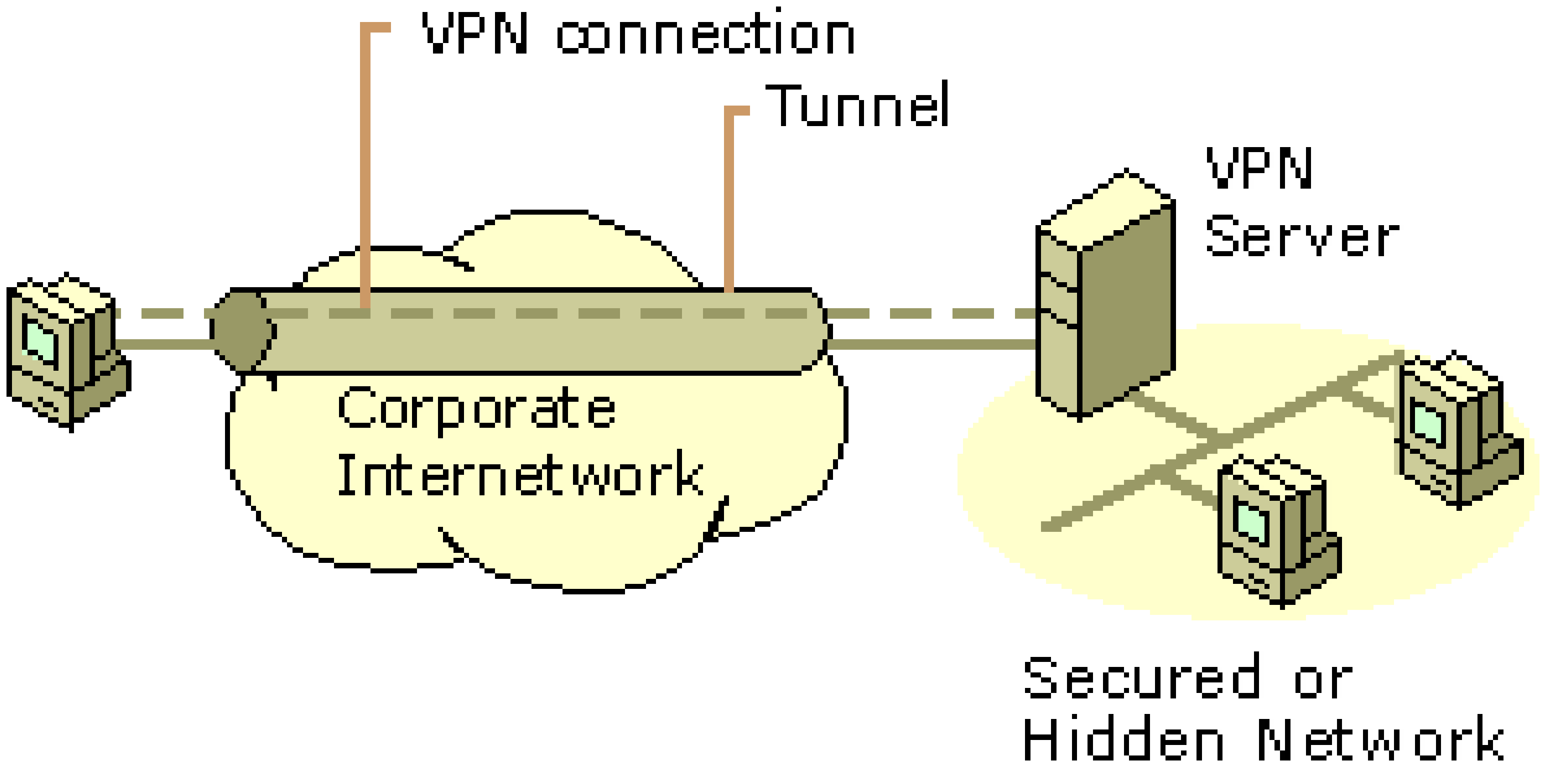
2. Connecting Networks Over the Internet (Site to Site VPN)



Virtual Private Networking: An Overview | Microsoft Docs

Common Uses of VPNs (3/3)

3. Connecting Computers over an Intranet (similar to 1.)



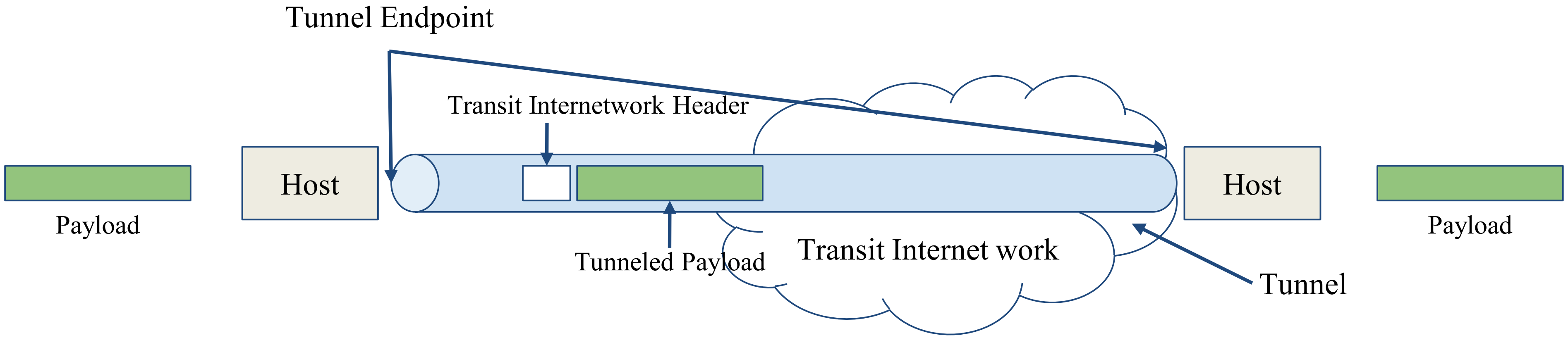
[Virtual Private Networking: An Overview | Microsoft Docs](#)

Why Use VPN?

- Cheap
  - Legacy private network uses remote connectivity through dial-up modems or through leased line connections, it’s expensive.
- Scalable
  - Extending a leased line connection is complex.
  - Easy to administer.
- Security
  - Provide encryption and file integrity.

VPN Key Concept - Tunneling

- VPN consists of a set of point to point connections tunneled over the Internet.
- In order to achieve tunneling, the packets are encapsulated as the payload of packets.
    - Payloads, to and from addresses, port numbers and other standard protocol packet headers
    - As seen by the external routers carrying the connection



Basic VPN Requirements

- User Authentication
- Key Management
- Address Management
- Data Encryption

Basic VPN Requirements (1/2)

- User Authentication
  - Verify the VPN client's identity and restrict VPN access to authorized users only.
  - Provide audit and accounting records to show who accessed what information and when.
  - X.509, pre-shared key, etc.
- Key Management
  - Generate and refresh encryption keys for the client and the server.
  - Simple Key Management for IP: ISAKMP/Oakley, etc.

Basic VPN Requirements (2/2)

- Address Management
  - Assign a VPN client's address on the intranet and ensure that private addresses are kept private
- Data Encryption
  - No one outside the VPN can alter the VPN.
  - Data carried on the public network must be rendered unreadable to unauthorized clients on the network.

VPN Security

- Authentication
  - Ensuring that the data originates at the source that it claims.
- Access Control
  - Restricting unauthorized users from gaining admission to the network.
- Confidentiality
  - Preventing anyone from reading or copying data as it travels across the Internet.
- Data Integrity
  - Ensuring that no one tampers with data as it travels across the Internet.

Common Implementations

- Based on PPP
  - Point-to-Point Tunneling Protocol (PPTP) (PPP + encryption + GRE)
  - Layer Two Tunneling Protocol (L2TP) (PPTP + L2F)
- Based on TCP/IP
  - L2TP/IPsec
  - IPsec Tunnel mode [RFC 4301]
  - BGP/MPLS IP VPN [RFC 4364]
- SSL/TLS
  - Secure Socket Tunneling Protocol (SSTP) (PPTP + SSL)
  - SSL VPN
  - OpenVPN

PPP - Point-to-Point Protocol

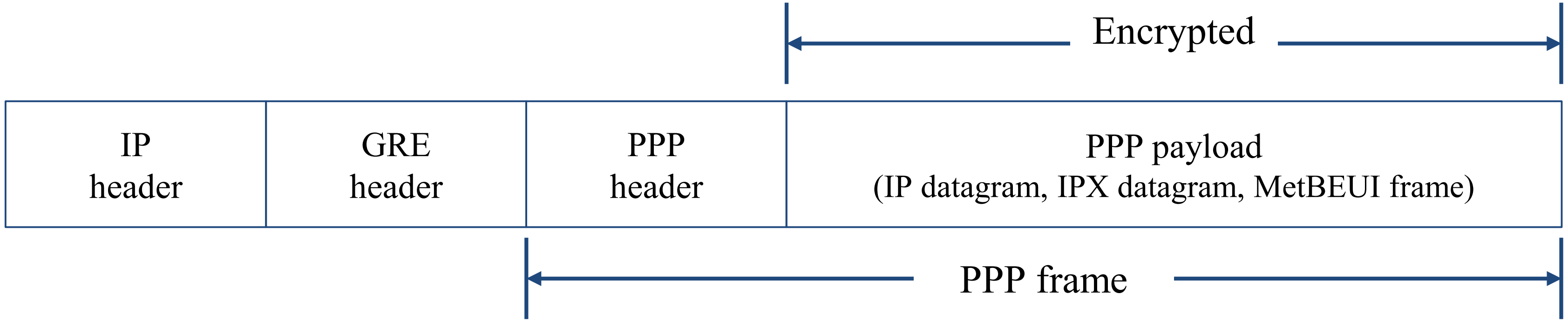
- PPP [RFC 1661] provides a standard method for transporting multi-protocol datagrams over point-to-point (direct) links.
    - Data link layer (layer 2) protocol
- Three components
    - Encapsulation (for transporting purpose)
    - Link Control Protocol (for data-link connectability)
    - Network Control Protocols (NCP) family (L3 management support)
- Extra Options
    - Authentication: PAP, CHAP, EAP, MS-CHAP, MS-CHAPv2, etc.
    - Link Quality and error detection
    - Compression
    - Encryption: MPPC + MPPE, etc.
    - Multilink (MP, The PPP Multilink Protocol)

Tunneling Protocol

- Allows a network user to access or provide a network service that the underlying network does not support or provide directly. (Wikipedia)
- GRE (Generic Routing Encapsulation): Establish a virtual point-to-point connection between two networks.
  - IP as a delivery protocol
  - Virtual Tunnel: (Tunnel) IP header + GRE packet header
  - Encapsulation, not encryption
- PPTP / L2TP
- IPsec
- OpenVPN (with SSL/TLS)
- etc.

PPTP - Point-to-Point Tunneling Protocol

- PPTP [RFC 2637] uses an enhanced GRE mechanism to provide a flow- and congestion-controlled (TCP) encapsulated datagram service for carrying PPP packets.
- PPTP creates a GRE tunnel through which the PPTP GRE packets are sent.

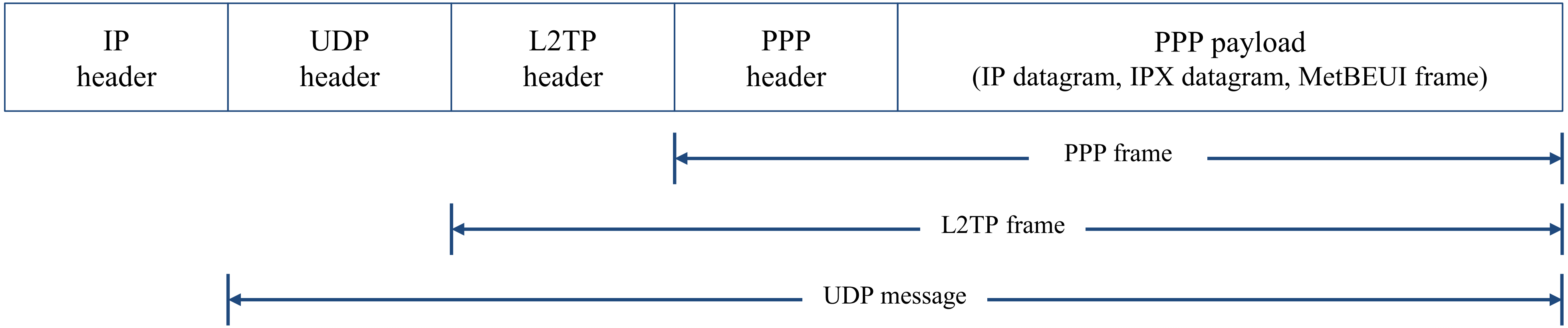


Security of PPTP

- PPTP has been the subject of many security analyses and
- serious security vulnerabilities have been found
  - MS-CHAP is fundamentally insecure.
  - MS-CHAPv2 is vulnerable to dictionary attack on the captured challenge response packets.
- The PPP payload can be encrypted by using Microsoft Point to Point Encryption (MPPE) when using MS-CHAPv1/v2
- EAP-TLS (Extensible Authentication Protocol – TLS) is the superior authentication choice for PPTP.

L2TP - Layer Two Tunneling Protocol

- L2TP [RFC 2661]: PPTP + L2F (Layer Two Forwarding)
- High level protocols (e.g., PPP) establish L2TP session ("call") within the L2TP tunnel, and traffic for each session is isolated.
- A tunnel can contains multiple connections at once.
- L2TP over IP internetworks uses UDP and a series of L2TP messages for tunnel maintenance.
- L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network. (Wikipedia)



IP header

UDP header

L2TP header

PPP header

PPP payload (IP datagram, IPX datagram, MetBEUI frame)

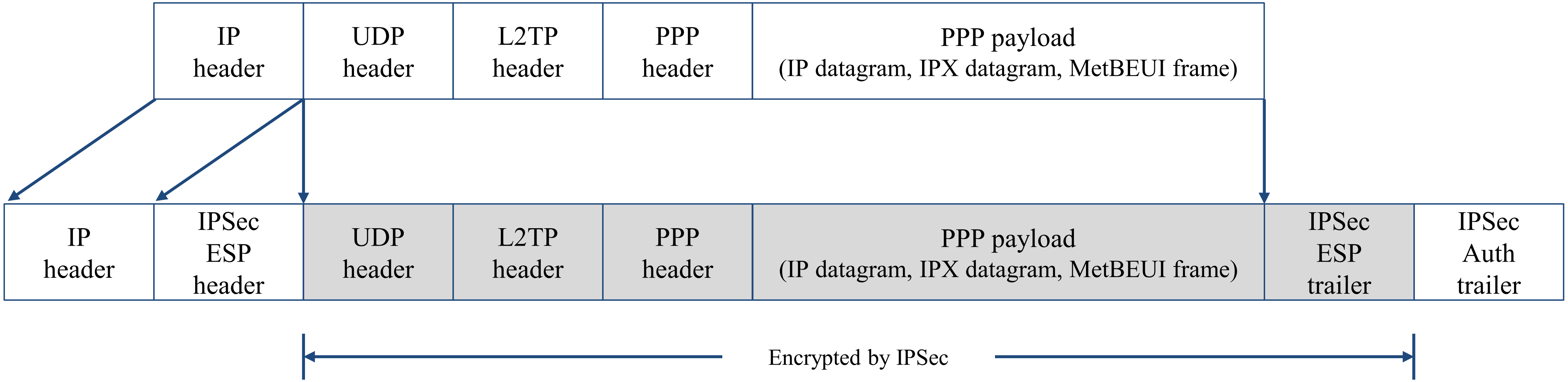
PPP frame

L2TP frame

UDP message

L2TP/IPsec

- L2TP does not provide confidentiality or strong authentication.
- Usually use IPsec ESP (Encapsulating Security Payload) to encrypt the L2TP packet.
  - Data encryption begins before the PPP connection process by negotiating an IPSec security association.
  - Require computer-level authentication using computer certificates.



IP header	UDP header	L2TP header	PPP header	PPP payload (IP datagram, IPX datagram, MetBEUI frame)

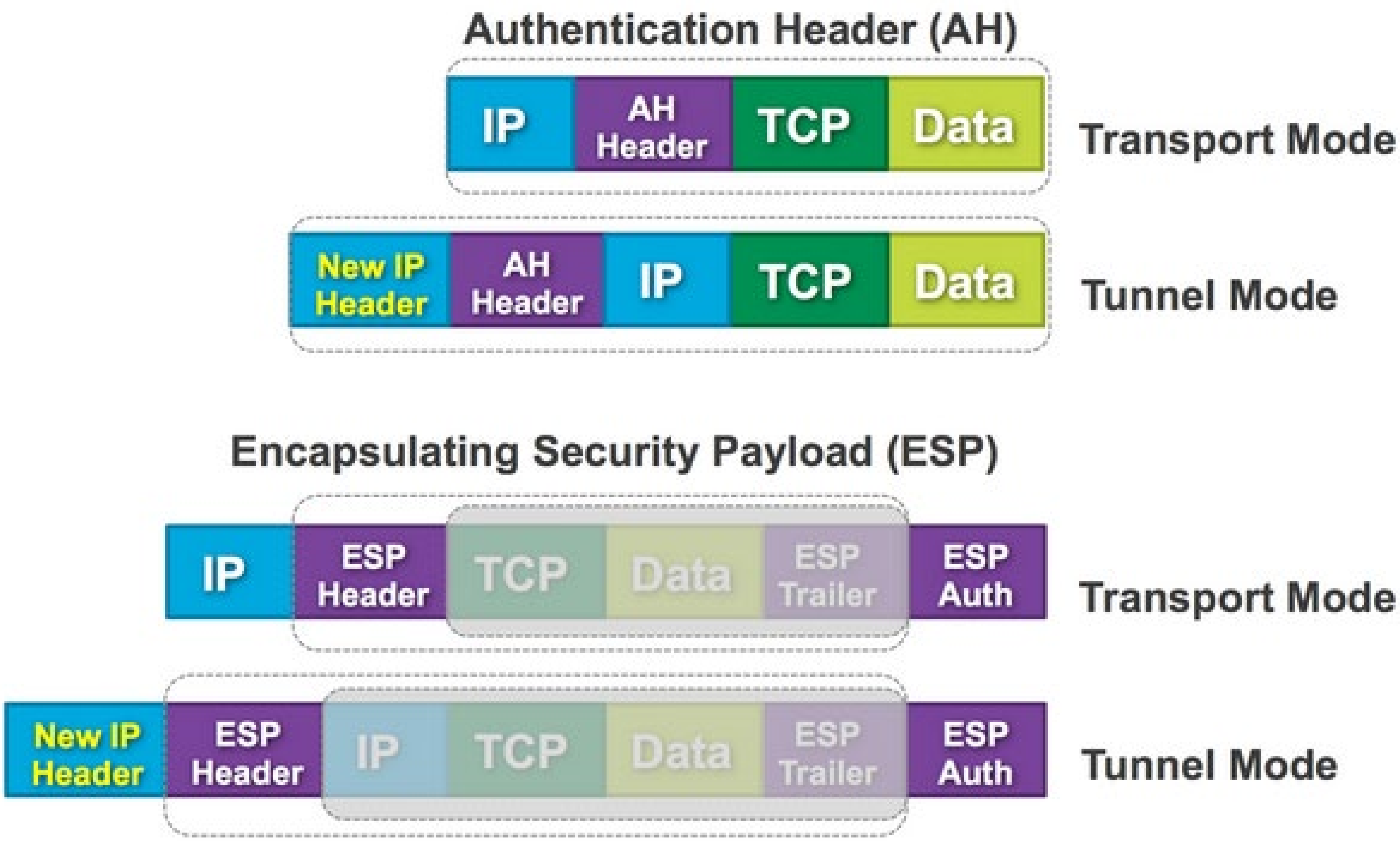
IP header	IPSec ESP header	UDP header	L2TP header	PPP header	PPP payload (IP datagram, IPX datagram, MetBEUI frame)	IPSec ESP trailer	IPSec Auth trailer

Encrypted by IPSec

IPsec

- IPsec [RFC 4301] is a secure network protocol suite provides authentication and encryption ability over IPv4 network.
- Two modes in IPsec
  - **Transport mode**: Insert IPsec header (AH/ESP) between IP and TCP header, then modify original IP header.
  - **Tunnel mode**: Encapsulate original packet, and prepend new IP and IPsec header.
- Two functions that ensure confidentiality:
  - Authentication Header (AH)
    - Provide source authentication and integrity without encryption.
  - Encapsulating Security Payload (ESP)
    - Provide both data authentication, data integrity and data encryption.
- Security Associations (SA) provides the parameters necessary for AH and/or ESP operations.
  - IKE (Internet Key Exchange): Provide authentication and key exchange. e.g., ISAKMP, OAKLEY

IPsec Modes



IPsec VPN Theory | Cisco Routing & Switching and Security (jazier.blogspot.com)

SSL VPN

- A form of VPN that can be used with a standard Web browser.
  - Also can be used to tunnel traffic via SSL or TLS protocol
- The traffic is encrypted with the SSL protocol or Transport Layer Security (TLS) protocol.
- Proprietary software
  - Cisco AnyConnect
  - Juniper Networks Pulse Secure
  - Fortigate
- Open Source
  - OpenVPN

Appendix

- I Am Anonymous When I Use a VPN – 10 Myths Debunked
- Virtual Private Networking: An Overview
- BeyondCorp by Google: Protected connection from untrusted networks without the use of a VPN.
    - See also: Role-Based Access Control (RBAC)
- Protocol reference
    - VPN
    - PPP / GRE / PPTP / L2TP
    - IPsec / IKE
    - IP protocol numbers